AMENDMENTS TO THE SPECIFICATION

Please amend the specification as indicated hereafter. It is believed that the following amendments and additions add no new matter to the present application.

In the Title:

Please replace the title with the following new title:

AUTHENTICATION METHOD IN A PRINTING ENVIRONMENT

In the Specification: [Use ~~strikethrough~~ for deleted matter (or double square brackets "[[]]" if the strikethrough is not easily perceivable, *i.e.*, "4" or a punctuation mark) and underlined for added matter.]

Please amend the paragraph starting on p. 10, line 27 as follows:

The unique identifier is preferably an alphanumeric code and the device preferably further comprises an input module for inputting the code to access the relevant entry in the audit log. This enables stored information about a particular printed out document to be obtained by use of the unique identifier ~~on~~ printed on the document itself. There is no need to have the document present, only the identifier is required. This also enables the exact machine from which a document originated to be identified, such that any further details regarding the document stored at the machine can be accessed.

Please amend the paragraph starting on p. 11, line 13 as follows:

It is often the case that fax numbers of certain fax machines are only available to several people within an organisation as those fax machines should only [[to]] be used for communications from specified sources. However, it is often difficult to ensure that only specified sources will transmit to the fax machine and proving the identity of the source has not been possible before.

Please amend the paragraph starting on p. 11, line 13 as follows:

Once the sending fax machine 14 has created the encrypted version 24 of the scanned-in document 12 and has obtained the digital certificate 18 of the intended recipient, then it can be sent to the receiving fax machine 16 together with the encrypted session key 25. However, prior to sending the information, the sending fax machine 14 implements a

modified interconnect fax protocol to establish the link between the two machines. The modification over the standard interconnect fax protocol is that the sending fax machine 14 inquires as to whether the receiving fax machine 16 is of the type which can be used according to the present embodiment, namely one which has the capability to stop the faxed document from being printed out until the intended recipient has proved their identity. If the receiving fax machine 16 is a standard machine, this is determined at this stage and the sending fax machine 14 can either not send the fax document 24 or send it as a normal non-encrypted fax, namely without the certificate 18 and session key 25, which will be printed out conventionally. However, if the receiving lax machine 16 is capable of implementing the present invention, then the next stage is to send at 50 the encrypted fax document 24, the intended recipient's certificate 18 and the encrypted session key 25 to the receiving fax machine 16.

Please amend the paragraph starting on p. 15, line 26 as follows:

For each public key 20 stored in the LDAP database 22, there is a corresponding single private key 26 which is owned by the individual themselves. This private key 26 is provided on an intelligent portable store such as a smart card 28, which the individual keeps personal possession of. The smart card 28 not only contains the private key 26, but also an algorithm for encoding or decoding data using the private key 26. The private key 26 enables the intended recipient to uniquely identify themselves to the receiving fax machine 16 in order to ~~received~~ receive the fax document 24, as will be described in detail later.

Please amend the paragraph starting on p. 18, line 8 as follows:

Referring now to Figure 2b, the process of receiving the fax document 24 and providing it to the intended recipient is now described. The receiving fax machine (RFM) 16 receives at 52 the encrypted fax document 24, the intended recipient's certificate 18 and the encrypted session key 25, and places these in the store 30. The receiving fax machine 16 then requests at 54 the intended recipient to input their smart card 28 (containing their private key 26) into the smart card reader 32. More specifically, this is carried out by the certificate 18, which contains the name of the intended recipient, being extracted from the received information and the name being displayed on the receiving fax machine 16. However, it is to be appreciated there are various different viable ways in which the intended recipient could be notified that there is a fax for them.

Please amend the paragraph starting on p. 20, line 1 as follows:

The receiving fax machine 16 is programmed to store each of the received certificates 18 and to request each of the intended recipients of the group to prove their identity to the receiving fax machine 16 by presentation of their respective smart cards 28 possibly within a given time period. More specifically, each of the members of the group is asked in turn to present their smart keys 28 to the receiving fax machine 16 to decrypt the multiple encrypted session key 25. The decryption is carried out on the smart card 28 itself as described previously. The order in which the members need to present their smart cards 28 to the receiving fax machine 16 is the reverse of the order for encoding the session key 25, namely starting with the last member of the group and finishing with the first. Also the decrypted result received from one member's smart card 28 is provided as the input to the next member's smart card 28 until such time as the multiple layers of encryption of the session key 25 has all been decrypted. At the end of this process, the session key 25 is decrypted correctly and can then be used to decrypt ~~and~~ the received fax document 24 for printing out. Accordingly, all of the intended recipients (members of the group) have to be present to enable the fax document 34 to be accessed.

Please amend the paragraph starting on p. 24, line 26 as follows:

If these two digests are equivalent from the comparison at 128, then the process continues and determines at 132 whether validation of the sender's certificate is required. If no validation is required, then the second part 120 of the process ends at 134 with the result that sender of the document and its contents can both be relied upon. This result is then identified to the recipient by the printing at 136 of a verifying mark (not shown) on the printout 34 of the received document 24. However, if validation is required as determined at 132, then the receiving fax machine 74 takes steps at <u>138</u> to check the validity of the certificate 18 or a chain of certificates of which the present certificate forms a part. These checks can be made on-line to higher and higher authorities and may, if necessary, extend all the way to a trusted authority such as Verisign. The process of on-line authentication of a certificate is well understood in the art and does not require further explanation herein.

Please amend the paragraph starting on p. 27, line 17 as follows:

The received NonceA is encrypted at 170 using C's private key (only available at C). This can be carried out on a smart card which holds the private key 159 as well as [[a]] an encoding/decoding algorithm for example. C then generates a new nonce (labeled as NonceC) and sends this at 172 together with the encrypted NonceA and C's digital Certificate to A.

Please amend the paragraph starting on p. 27, line 27 as follows:

A then decodes at 178 the encrypted NonceA using Cs public key (the Public key is either obtained from Cs Certificate or has previously been stored in A's memory. The decrypted version of NonceA is compared at 178 to the previously stored version of NonceA. If both versions are not equivalent at 180, then an irregularity in the authentication procedure has been detected and the subsequent transmission of a fax document between A and C is prevented at 168. Conversely, if both ~~version~~ versions are equivalent at 180, then A has proved that ~~that~~ the party who has sent the encrypted NonceA is the owner of C's private key, namely C and so commences its response procedure.

Please amend the paragraph starting on p. 28, line 8 as follows:

The response procedure commences at 182 with A encrypting the received NonceC with its own private key 159., Again the private key 159 may be provided on a smart card as in the previous embodiments. A then sends at 184 the encrypted NonceC to C. On receipt, C decodes at 18G the encrypted NonceC using A's public key (available via A's digital Certificate or previously stored) and compares this at 186 with the previously stored version of NonceC. If at 188 the decrypted version of NonceC is not equivalent to the stored original, then an irregularity in the authentication procedure 160 has been detected and the subsequent transmission of a fax document between A and C is prevented at 168. Otherwise, if both ~~version~~ versions are equivalent at 188, then C has proved that ~~that~~ the party who has sent the encrypted NonceC is the owner of A's private key 159, namely A. Accordingly, the authentication procedure 160 is now complete and the document can be faxed at 190 between A and C.

In the Abstract: [Use strikethrough for deleted matter and underlined for added matter.]

Please replace the pending abstract with the newly-submitted abstract attached herewith on a separate sheet.

Please amend the paragraph starting on p. 28, line 20 as follows:

The use of certificates 156 in the above procedure not only enables a local check to be made as to the membership of the closed group of the fax machine 152 wishing to commence communication but also enables each fax machine 152 to carry out on-line authentication checks to establish as an additional check whether each participating fax machine 152 is who it claims to be. Also this on-line authentication procedure provides an up-to-date validity check on the status of the fax machines' Certificates 156 if required.